

Ю. В. Харчейкина
старший прокурор отдела методической
и аналитической работы управления Генеральной прокуратуры
Республики Беларусь по надзору за соответствием закону
судебных решений по уголовным делам

О НЕКОТОРЫХ АСПЕКТАХ КРИМИНОЛОГИЧЕСКОЙ ХАРАКТЕРИСТИКИ КОМПЬЮТЕРНОГО САБОТАЖА

Компьютерный саботаж впервые криминализован законодателем в Уголовном кодексе Республики Беларусь (далее – УК), принятом в 1999 г. и введенном в действие с 1 января 2001 г. Опасность данного преступления в условиях информационного общества велика и все больше возрастает в связи с ростом различных способов использования компьютерных систем и сетей, что происходит в условиях активного развития технологий электронных платежей, возрастанием электронного документооборота, увеличением роли информации в жизни общества.

Уголовным законом Республики Беларусь компьютерный саботаж определен как умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (ч. 1 ст. 351 УК).

Первый пример привлечения к уголовной ответственности по рассматриваемой статье появился уже на следующий год после криминализации деяния.

Так, приговором суда Железнодорожного района г. Гомеля от 6 июня 2002 г. по ч. 1 ст. 351 УК осужден инженер-программист Республиканского унитарного предприятия «Гомельский завод сельскохозяйственного машиностроения «Гомсельмаш». Суд установил, что он в течение срока обязательной работы по распределению после окончания учебного заведения, желая добиться увольнения, изменил пароль доступа к корпоративной информации на сервере баз данных завода, в результате чего блокировал систему управления на файл-сервере предприятия и иные сетевые администраторы в течение десяти дней не смогли выполнять возложенные на них служебные обязанности. Допрошенный в ходе судебного заседания обвиняемый пояснил, что в обмен на пароль он хотел получить перевод на другую работу.

Основной тенденцией компьютерной преступности в целом и рассматриваемого состава в частности является ее постоянный рост, даже на фоне снижения уровня преступлений общеуголовной направленности.

Результаты проведенного Генеральной прокуратурой Республики Беларусь в 2015 г. обобщения следственно-судебной практики по уголовным делам о преступлениях, связанных с использованием компьютерных сетей, свидетельствуют, что за последние 10 лет количество зарегистрированных в республике преступлений, предусмотренных ст. 351 УК, увеличилось более чем в 16 раз (с 9 в 2006 г. до 146 в 2015 г.). Темп такого роста не замедляется (в 2012 г. зарегистрировано на 20 % преступлений больше к уровню предшествующего периода, 2013 г. – на 54 %, 2014 г. – на 124 %, 2015 году – на 75 %).

В то же время количество осужденных за компьютерный саботаж на протяжении всего действия уголовного закона остается относительно стабильным и незначительным (в среднем ежегодно – от 2 до 8 человек). В 2012 г. в совершении преступления, предусмотренного ст. 351 УК, признаны виновными 4 лица, в 2013 г. – 3, в 2014 г. – 6, в 2015 г. – 6. При этом отмечается ежегодное увеличение числа уголовных дел, производство по которым органом следствия приостановлено за неустановлением лица, подлежащего привлечению в качестве обвиняемого.

Такая ситуация свидетельствует о наличии определенных проблем в выявлении, раскрытии, расследовании и квалификации этого вида преступлений. Эти проблемы многообразны и обусловлены как трансграничным характером преступлений, техническими моментами производства оперативно-розыскных и процессуальных действий, фиксации электронной информации, получения, исследования доказательств, подтверждения их аутентичности, так и фрагментарностью, противоречивостью формулировок действующего законодательства в сфере информационной безопасности, их бланкетностью, влиянием положений других отраслей законодательства на применение указанной уголовно-правовой нормы.

Отсутствуют единообразные подходы и при квалификации подобных действий в следственно-судебной практике. Компьютерный саботаж в ряде случаев рассматривался как разновидность несанкционированного доступа к компьютерной информации, в других – эти действия оценивались как совокупность преступлений. Имеют место случаи возбуждения уголовных дел как отдельно по ст. 351 УК или ст.354 УК, так и по совокупности со ст. 208, 209 или 212 УК.

Расследование компьютерных преступлений осложняется отсутствием нормативного разъяснения узкоспециальных технических терминов гл. 31 УК, а также официального толкования Верховного Суда Республики Беларусь о применении норм УК, предусматривающих ответственность за преступления против информационной безопасности.

Отмеченный рост числа рассматриваемых преступлений связан с участвовавшими случаями блокирования с помощью вредоносных программ работы операционных систем компьютеров, сопровождающегося требованием злоумышленников об оплате их услуг по восстановлению работоспособности персональной электронной вычислительной машины, либо

случаями блокирования интернет-браузера от имени МВД с предложением уплатить штраф за мнимое правонарушение в сфере оборота порнографических материалов. Опыт борьбы правоохранительных органов Республики Беларусь с преступлениями против информационной безопасности свидетельствует, что, несмотря на относительно легкий способ их совершения, раскрываются они крайне трудно. Факты же осуждения лиц за такие деяния единичны.

Среди осужденных по ст. 351 УК значительный удельный вес занимают осужденные за деяния, совершенные в отношении информации интернет-или внутренних ресурсов своих же нанимателей, персональных аккаунтов локальных и социальных сетей, программ мгновенных сообщений, электронных почтовых ящиков знакомых либо членов семьи и т. п. При этом изучение рассмотренных судами уголовных дел показало, что в большинстве случаев осужденными совершены достаточно простые в техническом плане преступления и, как правило, ими не предпринимались меры к сокрытию следов преступления. Для совершения противоправных деяний виновными использовались чаще всего средства, созданные другими лицами и полученные посредством сети Интернет.

Мотивы такой преступной деятельности многообразны: безделье, вандализм, стремление доказать свои возможности и превосходство над техникой, исследовательский интерес, любопытство, извлечение личной или финансовой выгоды, месть, развлечение, самовыражение, честолюбие.

Так, например, приговором суда Заводского района г. Минска от 22 мая 2014 г. по ч. 1 ст. 351 и другим статьям УК осужден бывший работник ООО «ЕвроРеспектТехно». Он признан виновным в том, что, будучи уволенным за прогулы, используя идентификаторы доступа администратора, полученные в период работы в качестве помощника инженера-программиста, совершил несанкционированный доступ к информации сайтов предприятия и из мести удалил не менее 139 385 файлов.

Большинство осужденных в период с 2011 по 2015 гг. за преступления против информационной безопасности (ст. 349–355 УК) – мужчины (89 %). Для субъектов этих преступлений характерен высокий уровень образования: 37 % из них имели высшее и незаконченное высшее образование, 37 % – среднее специальное, 8 % – профессионально-техническое или общее среднее.

Осужденные за преступления против информационной безопасности характеризуются достаточно стабильным социальным статусом. На момент совершения преступления 70 % лиц работали. Большинство из них по месту работы и жительства характеризовались положительно. К этим осужденным не относятся такие криминогенные факторы, как пьянство (алкоголизм) и наркомания, характерные для лиц, совершивших преступления против личности, общественного порядка или хищения. На момент совершения компьютерного преступления возраст 43 % виновных не превышал 24 лет.

Данные показатели социально-демографической характеристики осужденных за преступления против информационной безопасности иллюстрируют в целом и «портрет» лиц, совершивших компьютерный саботаж.

Таким образом, в силу широкого использования компьютерной техники во многих сферах деятельности, многообразия способов и видов компьютерных преступлений в целях успешного выявления и пресечения противоправных деяний в рассматриваемой сфере представляется необходимым совершенствование уголовно-правовых основ противодействия преступности против информационной безопасности в целом и компьютерному саботажу в частности.